VIII kadencja

SEJM RZECZYPOSPOLITEJ POLSKIEJ

KANCELARIA SEJMU
Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ **Komisji Obrony Narodowej**
(nr 110)
z dnia 8 listopada 2018 r.

Pełny zapis przebiegu posiedzenia

Komisji Obrony Narodowej (nr 110)

8 listopada 2018 r.

Komisja Obrony Narodowej, obradująca pod przewodnictwem posła **Michała Jacha (PiS)**, przewodniczącego Komisji, zrealizowała następujący porządek obrad:

– rozpatrzenie informacji ministra obrony narodowej na temat procesu budowy kwalifikacji i gotowości do działań w obszarze cyberprzestrzeni;

– sprawy bieżące.

W posiedzeniu udział wzięli: **Wojciech Skurkiewicz** sekretarz stanu w Ministerstwie Obrony Narodowej wraz ze współpracownikami, **Paweł Dziuba** zastępca dyrektora Narodowego Centrum Kryptologii, mjr **Borys Iwaszko** przedstawiciel Służby Kontrwywiadu Wojskowego, **Joanna Maj-Mariańska** oraz **Michał Grzelak** z Departamentu Prawa i Bezpieczeństwa Pozamilitarnego Biura Bezpieczeństwa Narodowego oraz **Emilia Kunikowska** asystentka przewodniczącego Komisji.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Michał Madaj, Jacek Zientarski** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Michał Jach (PiS):

Dzień dobry państwu. Otwieram posiedzenie Komisji Obrony Narodowej.

Tematem dzisiejszego posiedzenia jest rozpatrzenie informacji ministra obrony narodowej na temat procesu budowy kwalifikacji i gotowości do działań w obszarze cyberprzestrzeni.

Stwierdzam kworum oraz przyjęcie protokołu ze 109. posiedzenia Komisji, wobec niewniesienia do niego zastrzeżeń.

Jeżeli nie usłyszę sprzeciwu uznam, że przyjęliśmy porządek dzienny. Sprzeciwu nie słyszę.

Witam zaproszonych gości. Witam pana ministra Wojciecha Skurkiewicza sekretarza stanu w Ministerstwie Obrony Narodowej. Witam pana pułkownika Marka Gładysza zastępcę szefa Zarządu Kierowania i Dowodzenia P-6 Sztabu Generalnego Wojska Polskiego, pana Pawła Dziubę zastępcę dyrektora Narodowego Centrum Kryptologii, pana pułkownika Tomasza Żyto zastępcę szefa Inspektoratu Informatyki, pana majora Borysa Iwaszko przedstawiciela Służby Kontrwywiadu Wojskowego, panią Joannę Maj-Mariańską oraz pana Michała Grzelaka z Departamentu Prawa i Bezpieczeństwa Pozamilitarnego w Biurze Bezpieczeństwa Narodowego.

Proszę państwa, dzisiejszy temat jest związany z realizacją planu pracy Komisji na II półrocze bieżącego roku. Państwo posłowie otrzymali materiały dotyczące dzisiejszego tematu. W związku z powyższym proszę pana ministra o przedstawienie informacji.

Sekretarz stanu w Ministerstwie Obrony Narodowej Wojciech Skurkiewicz:

Bardzo dziękuję, panie przewodniczący. W związku z tym, że te informacje dotarły do państwa posłów, bardzo proszę o przedstawienie szczegółowych informacji zastępcę dyrektora Narodowego Centrum Kryptologii pana Pawła Dziubę, który wyjaśni wszystkie nurtujące państwa kwestie.

Przewodniczący poseł Michał Jach (PiS):

Bardzo proszę, panie dyrektorze.

Zastępca dyrektora Narodowego Centrum Kryptologii Paweł Dziuba:

Dziękuję bardzo, panie ministrze. Szanowny panie przewodniczący, Wysoka Komisjo, szanowni państwo, przedstawię jawną informację na temat procesu budowy kwalifikacji i gotowości do działań w cyberprzestrzeni. Zdolność do skutecznej ochrony zasobów informacyjnych, a w szczególności istotnych i krytycznych dla bezpieczeństwa państwa, stanowi ważny wyznacznik nowoczesności państwa w dobie postępującej cyfryzacji oraz rosnącego, cywilizacyjnego uzależnienia od technologii cyfrowych. Ministerstwo Obrony Narodowej, dostrzegając rosnące wyzwania i zagrożenia dla bezpieczeństwa cyberprzestrzeni Polski, uznało ten obszar działań za jeden z priorytetowych, co zostało przedstawione i obejmuje wiele przedsięwzięć podjętych przez kierownictwo Ministerstwa Obrony Narodowej. Znalazło to potwierdzenie m.in. w działalności Narodowego Centrum Kryptologii, jak również Służby Kontrwywiadu Wojskowego, Sztabu Generalnego Wojska Polskiego, a zwłaszcza Zarządu P-6 oraz Inspektoratu Informatyki.

Podnoszenie zdolności Sił Zbrojnych Rzeczypospolitej Polskiej do prowadzenia działań militarnych w cyberprzestrzeni realizowane jest w szerokich aspektach, obejmujących m.in. prace koncepcyjne nad powołaniem Wojsk Obrony Cyberprzestrzeni i określeniem ich kompetencji. Wymóg utworzenia Wojsk Obrony Cyberprzestrzeni jest w interesie polskiej racji stanu, jak też zgodny ze zobowiązaniami podjętymi na szczycie NATO w Warszawie, na którym zadeklarowaliśmy, że cyberprzestrzeń jest kolejną domeną operacyjną. Ustalenia te obligują Rzeczpospolitą Polską do podjęcia wysiłku zmierzającego do posiadania zdolności prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni, a tym samym dysponowania środkami odstraszania i zapobiegania potencjalnym cyberatakom.

Głównym zadaniem Wojsk Obrony Cyberprzestrzeni jest wykrywanie, rozpoznawanie i zapobieganie cyberzagrożeniom, wsparcie, ochrona oraz obrona sieci i systemów teleinformatycznych, prowadzenie cyberrozpoznania, wsparcie operacji militarnych prowadzonych przez siły zbrojne w cyberprzestrzeni. Ponadto ich zadaniem jest m.in. planowanie i prowadzenie działań militarnych w cyberprzestrzeni w wymiarze narodowym, jak również zapewnienie wsparcia operacji militarnych prowadzonych przez Siły Zbrojne Rzeczypospolitej Polskiej. W Ministerstwa Obrony Narodowej finalizowane są prace nad projektem decyzji o formowaniu Wojsk Obrony Cyberprzestrzeni.

Kolejnym aspektem wpływającym na poziom zdolności w cyberprzestrzeni jest udział w systemie planowania i programowania rozwoju Sił Zbrojnych RP, w którym ujęte są wieloletnie perspektywy rozwoju systemów teleinformatycznych i systemów bezpieczeństwa teleinformatycznego w aspekcie organizacyjnym, finansowym, jak również technicznym. Kierunkowe ustalenia zapisane są w programie rozwoju w latach 2013–2022, jak również są uwzględniane w pracach kolejnego cyklu planistycznego programu rozwoju w latach 2017–2026. Istotnym aspektem wpływającym również na poziom zdolności w cyberprzestrzeni jest cyberobrona, w tym utworzenie CSIRT-MON. W siłach zbrojnych istnieje i funkcjonuje system reagowania na incydenty komputerowe. Jest on aktualizowany w wyniku wdrożenia ustawy o krajowym systemie cyberbezpieczeństwa. Trwa dostosowanie struktur resortu obrony narodowej odpowiedzialnych za bezpieczeństwo cyberprzestrzeni do wymogów ustawy, w tym prace nad nowelizacją decyzji w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej. Istotnym elementem wpływającym również na poziom bezpieczeństwa w cyberprzestrzeni jest prowadzenie innowacyjnych badań i rozwoju. W tym aspekcie kierownictwo Ministerstwa Obrony Narodowej zleciło konsolidację i intensyfikację badań naukowych realizowanych w obszarze kryptologii i cyberbezpieczeństwa.

W tym aspekcie ważny jest również rozwój narodowych zdolności w zakresie kryptologii, który zapewnia utrzymanie zdolności w zakresie wymaganego poziomu poufności informacji w systemach teleinformatycznych poprzez zastosowanie odpowiedniej techniki, urządzeń, oprogramowania. Sprawne zarządzanie kryptografią jest kluczowym filarem zapewnienia bezpieczeństwa teleinformatycznego w siłach zbrojnych. Obowiązujące ramy prawne stosowanych rozwiązań zapewniają ochronę narodowych informacji niejawnych oraz informacji sojuszniczych. W tym względzie organy wykonawcze zabezpie-

czenia kryptograficznego, którymi są komórki bezpieczeństwa systemu łączności i informatyki funkcjonujące w resorcie obrony narodowej na różnych poziomach dowodzenia – wiodącą jednostką jest Narodowe Centrum Kryptologii – zapewniają sprawne funkcjonowanie lokalnych systemów kryptograficznych. Narodowe Centrum Kryptologii, zgodnie ze swoim statutem, konsoliduje kompetencje i zasoby resortu obrony narodowej w obszarze kryptologii, a w szczególności określa kierunki rozwoju systemów kryptograficznych. Jako gestor urządzeń i narzędzi kryptograficznych koordynuje zabezpieczenie potrzeb sił zbrojnych w tym zakresie.

Podkreślić należy współpracę z krajowymi ośrodkami naukowo-badawczymi i krajowym przemysłem, czego materialnym wyrazem są prowadzone projekty naukowo -badawcze związane z obszarem narodowych technologii kryptograficznych. W tym zakresie prowadzone są prace, których celem jest opracowanie narodowych rozwiązań zabezpieczających informacje niejawne do poziomu klauzuli „ściśle tajne”. Istotnymi elementami, które również wpływają na poziom bezpieczeństwa w cyberprzestrzeni, są elementy związane z edukacją i ustawicznym kształceniem. W tym obszarze resort podejmuje wielokierunkowe działania, których celem jest posiadanie wysoko wykwalifikowanego personelu w dziedzinie informatyki, kryptologii i cyberbezpieczeństwa. Podkreślić należy, że w istniejącym systemie kształcenia w zakresie pozyskania kadr o specjalności informatyka, kryptologia i cyberbezpieczeństwo zwiększono limity przyjęć w uczelniach wojskowych. Ponadto personel pozostający w służbie kierowany jest na wysoko specjalizowane szkolenia zarówno w ośrodkach krajowych jak i zagranicznych, w tym na szkolenia organizowane przez Sojusznicze Centrum Eksperckie Cyberobrony NATO w Tallinie. Kontynuowany jest również proces edukacji dla kadry i pracowników wojska w zakresie bezpieczeństwa teleinformatycznego. W ramach tych działań prowadzone są przede wszystkim okresowe szkolenia. Prowadzone są wewnętrzne portale informacyjne poświęcone zagadnieniom bezpieczeństwa. Publikowane są biuletyny informacyjne z dziedziny bezpieczeństwa oraz komunikaty ostrzegawcze dla użytkowników systemów teleinformatycznych resortu obrony narodowej. W procesie szkolenia wykorzystywana jest również platforma nauczania na odległość – e-Learning.

Istotnym elementem, wpływającym również na poziom bezpieczeństwa w cyberprzestrzeni, jest prowadzenie współpracy z podmiotami krajowymi i zagranicznymi. W tym względzie chciałbym zauważyć, że Ministerstwo Obrony Narodowej prowadzi konsultacje bilateralne i multilateralne w obszarze cyberbezpieczeństwa w ramach Sojuszu Północnoatlantyckiego, ze szczególnym uwzględnieniem Stanów Zjednoczonych. Ministerstwo współdziała z zespołami reagowania na incydenty komputerowe w Polsce oraz z zespołem NATO CIRC, uczestniczy w pracach międzynarodowych grup roboczych w zakresie cyberbezpieczeństwa, kryptologii oraz rozwoju systemów i technologii teleinformatycznych, współpracuje z przedsiębiorcami telekomunikacyjnymi oraz podmiotami sektora prywatnego uczestniczącymi w realizacji infrastrukturalnych projektów na rzecz sił zbrojnych w dziedzinie IT i kryptologii.

Ważnym elementem jest również udział w krajowych i międzynarodowych ćwiczeniach z zakresu bezpieczeństwa teleinformatycznego oraz interoperacyjności systemów teleinformatycznych. Istotne ćwiczenie, w których biorą udział przedstawiciele naszych sił zbrojnych, to m.in. LOCKED SHIELD, CWIX, TTX US EUCOM, CYBER COALITION. Bardzo istotne jest również ćwiczenie Anakonda prowadzone pod auspicjami Polski, które jest przede wszystkim sprawdzeniem zdolności w tradycyjnych domenach działań militarnych. Od 2016 r. to ćwiczenie jest też dobrym przykładem współdziałania w zakresie bezpieczeństwa teleinformatycznego jednostek Sił Zbrojnych Rzeczypospolitej Polskiej oraz jednostek państw sojuszniczych. Tegoroczne ćwiczenia „Anakonda 18” pozwolą sprawdzić współdziałanie sił zbrojnych przy realizacji epizodów z realnymi zagrożeniami w cyberprzestrzeni. Ważne dla osiągnięcia zamierzonych celów, jeśli chodzi o zdolności w cyberprzestrzeni, jest realizacja programu operacyjnego osiągnięcia zdolności operacyjnej w zakresie bezpieczeństwa cyberprzestrzeni i wsparcia kryptologicznego. W programie opisano szczegółowe zadania związane z osiąganiem i utrzymaniem zdolności operacyjnych sił zbrojnych z zakresu bezpieczeństwa cyberprzestrzeni i wspo-

magania kryptologicznego. Szanowni państwo, ten dokument jest opatrzony klauzula tajności. Stąd omówienie go na jawnym posiedzeniu Komisji nie jest możliwe.

Ostatni element, o którym chciałbym wspomnieć, jest bardzo istotny, ponieważ posiadane narzędzia, posiadane zdolności muszą być wspierane przez ludzi, przez specjalistów. W tym aspekcie kierownictwo Ministerstwa Obrony Narodowej podjęło intensywną rekrutację na stanowiska w strukturach właściwych w zakresie obrony cyberprzestrzeni. Ministerstwo planuje zainicjowanie wielowymiarowej kampanii rekrutacyjnej skierowanej do osób chcących realizować swoje pasje i kwalifikacje w obszarze bezpieczeństwa cyberprzestrzeni w służbie dla ojczyzny, dla Polski. Preludium, to najbliższy HACKATON w ramach rządowej inicjatywy…, na którym pod patronatem ministra obrony narodowej będzie zorganizowany konkurs dla specjalistów z obszaru cyberbezpieczeństwa. Jeżeli są tym państwo zainteresowani, szczegóły dostępne są na stronie <hackaton.wp.mil.pl>.

Szanowna Komisjo, podsumowując, kierownictwo Ministerstwa Obrony Narodowej priorytetowo podchodzi do spraw dotyczących bezpieczeństwa systemów informatycznych i szeroko pojętego bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej. Dowodem tego jest wiele ze wspomnianych działań podejmowanych w resorcie obrony narodowej, jak również na forum NATO, a także ujęcie obszaru cyberprzestrzeni w Planie modernizacji technicznej sił zbrojnych. Na zakończenie chciałbym podkreślić, że nie bez znaczenia dla rozwoju sił zbrojnych do prowadzenia działań w cyberprzestrzeni jest również stworzenie warunków konkurencyjności w stosunku do rynku cywilnego dla poszukiwanych specjalistów w obszarze informatyki, cyberbezpieczeństwa i kryptologii. Jak wspomniałem, te działania są identyfikowane w Ministerstwie Obrony Narodowej. Szanowny panie przewodniczący, szanowni państwo, panie ministrze, dziękuję.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję. Proszę państwa, otwieram dyskusję. Zachęcam do zadawania pytań. Pan dyrektor przedstawił informację bardzo podobną do tej, którą otrzymaliśmy na piśmie. Jeśli są jakieś pytania dotyczące spraw bardziej szczegółowych, to proszę bardzo. Proszę bardzo, pan poseł Paweł Suski.

Poseł Paweł Suski (PO):

Dziękuję, panie przewodniczący. Wysoka Komisjo, chciałbym dopytać o przedstawiane na poziomie kierownictwa Ministerstwa Obrony Narodowej od 2016 r. plany dotyczące obrony cyberprzestrzeni. Pan dyrektor przedstawił założenia czy strukturę czynności podjętych z poziomu, którym kieruje. Natomiast my bierzemy również pod uwagę to, co robi kierownictwo Ministerstwa Obrony Narodowej, co zapowiadał i obiecywał w tej sprawie minister obrony narodowej Antoni Macierewicz. Myślę, że słynny „miliard" na obronę cyberprzestrzeni jest tutaj pewnym kluczem.

Mamy dzisiaj informacje o tworzeniu nowego rodzaju sił zbrojnych – Wojsk Obrony Cyberprzestrzeni. Pan dyrektor przedstawił, że jest to działanie koncepcyjne. W skrócie powiedział, na czym mniej więcej to polega. Mamy 3 lata w zakresie planowania i obietnic wrzuconych w przestrzeń przez poprzedniego ministra obrony narodowej. Mamy zapowiedź wydania 1 mld zł, a na poziomie Komisji tak naprawdę słyszymy o działaniach koncepcyjnych. Plan, który został przedstawiony – zresztą szeroko opisywany – dotyczył wielu zagadnień, m.in. realizacji czy implementacji systemu do analizy ruchu sieciowego typu NetFlow, co też wzbudzało różne emocje i kontrowersje. Chcę podkreślić, że obrona cyberprzestrzeni powinna być – tu zgadzam się z poprzednim ministrem – priorytetem ministerstwa. Ale po 3 latach tak naprawdę mamy ciągle malutką bańkę. Nie wiadomo, jak się ona rozwinie. Czy możemy mówić o szczegółach, o konkretach poziomu zabezpieczenia, poziomu bezpieczeństwa cybernetycznego, czy ciągle jest to tylko „mowa trawa"?

Przewodniczący poseł Michał Jach (PiS):

Proszę bardzo, pani poseł Bożena Kamińska.

Poseł Bożena Kamińska (PO):

Dziękuję bardzo, panie przewodniczący. Wysoka Komisjo, szanowni goście, panie ministrze, rozmawiamy o bardzo istotnej kwestii, która jest również często podnoszona

na sesjach Zgromadzenia Parlamentarnego NATO, że cyberbezpieczeństwo jest podstawą bezpieczeństwa państwa i społeczności w XXI wieku. Chcę przypomnieć, że – niestety – mamy odnotowane włamania do Ministerstwa Obrony Narodowej. Były dwa włamania. Jedno 30 listopada 2015 r., a drugie 28 lutego 2016 r. Wiadomo, że nastąpiło włamanie do prywatnych skrzynek pocztowych pracowników Ministerstwa Obrony Narodowej i Sztabu Generalnego Wojska Polskiego. Przejętych zostało co najmniej 1 tys. maili osób pracujących w wojsku. Wiemy, że atak prowadzony był z serwerów na Łotwie.

Bardzo ważne, istotne jest to, że mamy te programy. Natomiast, w mojej ocenie, przez cały czas jesteśmy w punkcie projektowania, analiz, szkolenia, edukowania i poszukiwania kadr. Nie mamy konkretnych środków, które służyłyby bezpieczeństwu w cyberprzestrzeni, w szczególności jeżeli chodzi o obiekty strategiczne obrony narodowej, jak również obiekty gospodarcze w naszym kraju. Mam kilka pytań. Kieruję je do pana ministra, chociaż to pan dyrektor przedstawiał szczegóły. Panie ministrze, pierwsze pytanie dotyczy tego, że jest podnoszone, że jest to temat priorytetowy. W takim razie, jak mają się prognozowane środki na cyberbezpieczeństwo i wsparcie kryptologiczne na 2019 r. w budżecie Ministerstwa Obrony Narodowej, w wysokości zaledwie 42 mln zł? W projekcie budżetu zabezpieczona jest jedynie taka kwota. Wcześniej były zapowiedzi dotyczące również stworzenia wojsk cybersec. Chcę wiedzieć, co państwo za te 42 mln zł w 2019 r. chcą wykonać? Jakie priorytety z tych planów zostaną zrealizowane za te środki finansowe? Nie chcę podawać przykładów czy porównań dotyczących tego, co w obszarze cyberprzestrzeni możemy wykonać za 42 mln zł.

Niezależnie od wielkości tego budżetu chciałabym zapytać, jak wygląda struktura cybersec kraju? Jakie jest na jej tle miejsce i rola Ministerstwa Obrony Narodowej? Kolejne pytanie dotyczy strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej, która została przyjęta w maju 2017 r. Wraz z nią został przyjęty plan działań na rzecz wdrożenia krajowych ram polityki cyberbezpieczeństwa. Są tam m.in. zadania dla Ministerstwa Obrony Narodowej. To wszystko jest zawarte w budżecie na przyszły rok, w którym będą 42 mln zł. Mam również pytanie, jakie konkretne zadania przypisane w tej strategii Ministerstwu Obrony Narodowej, zostaną zrealizowane przez resort w 2019 r. za 42 mln zł zaplanowane w budżecie Ministerstwa Obrony Narodowej? Dziękuję bardzo.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję. Pani poseł Anna Maria Siarkowska. Proszę.

Poseł Anna Maria Siarkowska (PiS):

Bardzo dziękuję. Panie przewodniczący, panie ministrze, Wysoka Komisjo, kwestia związana z walką w obszarze cyber jest warta rozważenia, jeżeli chodzi o utworzenie kolejnego rodzaju sił zbrojnych, bo rzeczywiście jest to kolejna przestrzeń walki. Jeśli mówimy o rodzajach sił zbrojnych, to mówimy o nich w kontekście przestrzeni walki, którą prowadzą. Wojska Lądowe, na lądzie. Siły Powietrzne, w powietrzu. Marynarka Wojenna, na terytoriach morskich. Rzeczywiście, sfera cyber pod względem logicznym wymagałaby utworzenia kolejnego rodzaju wojsk. Powiem szczerze, że – z tego, co pamiętam bezpośrednio po strategicznym przeglądzie obronnym – zadawałam to pytanie panu ministrowi Szatkowskiemu. Na forum Komisji Obrony Narodowej otrzymałam informację, że nie planuje się utworzenia oddzielnego rodzaju wojsk – Wojsk Cybernetycznych. Rozumiem, że od tego momentu nastąpiła w tym zakresie zmiana. Jestem gotowa to przyjąć.

Natomiast w związku z tym mam konkretne pytania. Specjalistów w tym obszarze już od pewnego czasu próbowano zgromadzić w wojskach operacyjnych. Problem, z którym się spotykano, polegał na tym, że płace dla specjalistów w obszarze cyber na wolnym rynku oscylują w widełkach od 9 do 15 tys. zł brutto. Tymczasem to, co proponowano tym specjalistom w wojsku, to widełki od 3 do 5 tys. zł brutto. W związku z tym pojawia się pytanie, w jaki sposób wojsko zamierza pozyskać takich specjalistów na pełny etat i czy znajdą się na to środki? To jest pierwsze pytanie. Drugie pytanie polega na tym, czy można do tego problemu podejść w troszeczkę inny sposób, jeśli są problemy związane z finansami? Mamy taką formę służby, jak terytorialna służba wojskowa. Gromadzi ona ludzi, którzy łączą służbę wojskową ze swoim normalnym, codziennym życiem zawo-

dowym. Może specjalistów, którzy na co dzień pracują w firmach komercyjnych, można byłoby pozyskać do tego, żeby jakąś część swojego czasu poświęcali również armii. Jest to kwestia do rozważenia. Uważam, że zasadniczym problemem jest to, czy wojsko, czy polskie siły zbrojne będzie stać na to, żeby utworzyć nowy rodzaj wojsk, rzeczywiście składający się z wysoko wykwalifikowanych specjalistów w tym obszarze i czy jesteśmy tutaj w stanie konkurować z rynkiem cywilnym, na którym pensje dla takich osób są znacznie, znacznie wyższe. Dziękuję.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję. Bardzo proszę, panie ministrze.

Poseł Joanna Kluzik-Rostkowska (PO):

Czy jeszcze mogę?

Przewodniczący poseł Michał Jach (PiS):

Czy są jeszcze jakieś pytania? Nie. W takim razie, proszę. Pani minister Joanna Kluzik -Rostkowska.

Poseł Joanna Kluzik-Rostkowska (PO):

Dziękuję bardzo. Swego czasu toczył się spór, ponieważ NATO uważało, że cyberwojsko miała pełnić głównie rolę ochronną, to znaczy, że wszystkie działania w cyberprzestrzeni miały służyć ochronie. Już w tym czasie Putin nie miał żadnych wątpliwości co do tego, że informacja, to jest broń. Putin w swojej doktrynie stwierdzenie, że informacja, to jest broń, zawarł już w 2000 r. Armia rosyjska też za tym poszła. Zdaje się, że 10 lat później przyznała, że informacja, to kolejny rodzaj broni. Za tym poszły fabryki trolli itd. W tym czasie na Zachodzie toczył się bardzo intensywny spór o to, czy informacja może być bronią, czy nie, czy w ogóle informację możemy traktować jako rodzaj broni zaczepnej. Oczywiście, chodzi tu również o dezinformację.

Chciałabym zapytać, jak państwo to widzą? Czy jesteście bliżsi temu, że informacja może być traktowana jako nowy rodzaj broni, szczególnie w kontekście Rosji, która nie ma co do tego żadnych wątpliwości, czy jednak trzymacie się standardów NATO, czyli traktowania tego wyłącznie pasywnie? Przy okazji chciałam wrócić do tego, o czym mówiła moja poprzedniczka. Przypomniałam sobie, że wiele lat temu był w polskim rządzie problem, który polegał na tym, że powstało Ministerstwo Rozwoju, w którym ludzie pracowali średnio po 9 miesięcy, ponieważ rynek potrzebował specjalistów od programów europejskich. Ci ludzie byli natychmiast wsysani przez rynek. Wtedy stworzyła się taka sytuacja, że to ministerstwo, jako jedyne, było znacznie lepiej opłacane niż inne ministerstwa. Wszyscy się z tym pogodzili. Uważam, że żeby to miało sens, musi być rzeczywiście bardzo dobrze opłacana kadra. W związku z tym trzeba mieć na uwadze jakieś ekstraordynaryjne przedsięwzięcia. Czy państwo zdają sobie z tego sprawę? Czy o tym myśleliście? Dziękuję.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję. Proszę bardzo, panie ministrze.

Sekretarz stanu w MON Wojciech Skurkiewicz:

Dziękuję bardzo. Panie przewodniczący, szanowni państwo, jeżeli chodzi o ostatnią kwestię poruszoną przez panią poseł Kluzik-Rostkowską, to za chwile pan major Iwaszko rozwieje wszelkie wątpliwości. Szanowni państwo, pani poseł Siarkowska zwracała uwagę na kwestie finansowe. Zdajemy sobie sprawę z tego, że w zderzeniu z rynkiem cywilnym jesteśmy mało konkurencyjni jako wojsko pod względem finansowym. Ale dzisiaj zwiększamy dodatki, które są tak, żeby równać do poziomu cywilnego. Nie jest prawdą, że to jest poziom od 3 do 5 tys. zł, bo dziś są to zdecydowanie wyższe środki finansowe, jeżeli chodzi o ten szczególnie wrażliwy obszar i o tych żołnierzy, funkcjonariuszy i pracowników, którzy w tym obszarze funkcjonują. Ta sytuacja będzie jeszcze sukcesywnie ulegała zmianie, czyli środki będą wzrastały. Zdajemy sobie sprawę, że jest to obszar na tyle wrażliwy, na tyle interesujący z punktu widzenia rynku cywilnego, że tych specjalistów – szczególnie wybitnych specjalistów, których mamy w polskim wojsku – musimy zatrzymać.

Dzisiaj stwarzamy również możliwości do tego, żeby tych specjalistów również pozyskiwać. Może wyjdę poza ustaloną sztampę posiedzenia Komisji. Dzisiaj jest tak, jeżeli chodzi o obszar cyber IT, że jeśli mamy problemy z pozyskaniem pracowników czy żołnierzy z wyższym wykształceniem, poszukujemy również kadry wśród osób, które mają średnie wykształcenie. Jeżeli ktoś jest wybitnym ekspertem, wybitnym specjalistą, to nie możemy mu powiedzieć, że go nie chcemy, bo nie ma wyższych studiów. Dzisiaj stwarzamy również takie możliwości, żeby zasysać z rynku cywilnego jak największą grupę dobrych i wybitnych fachowców. Oczywiście, względy finansowe są kluczowe. Zdajemy sobie wszyscy sprawę, że w tym obszarze trudno jest znaleźć osobę do pracy za 3 czy za 5 tys. zł – jak pani przywoływała – bo na rynku cywilnym jest ona w stanie uzyskać wielokrotnie więcej. Co do tego nie ma najmniejszej wątpliwości.

Szanowni państwo, nie zapominajmy o tym, że dzisiaj rozmawiamy o tym w sytuacji zdecydowania innej niż jeszcze kilka miesięcy temu, bo dziś – na szczęście – mam przyjęta ustawę o krajowym systemie cyberbezpieczeństwa. Nie powiem, że ta ustawa traktuje ten obszar w sposób perfekcyjny, ale w zupełnie inny niż jeszcze kilka czy kilkanaście miesięcy temu. Zdajemy sobie sprawę, że jest to obszar na tyle wrażliwy nie tylko z punktu widzenia Ministerstwa Obrony Narodowej, ale również innych ministerstw, z którymi została podjęta współpraca i w których to wyzwanie jest dzisiaj realizowane. 42 mln zł. Szanowni państwo, Narodowe Centrum Kryptologii, to budżet 111 mln zł. Do tego jest 700 mln zł z programów operacyjnych. Dziś mówimy o takich środkach finansowych, jeżeli mówimy np. o 2018 r.

Oczywiście, pani poseł, możemy mówić tak, że bierzemy zakładkę, w której są 42 mln zł. Ale takich zakładek w części 29 – Ministerstwo Obrony Narodowej, jest zdecydowanie więcej. Dodatkowo, w związku z ustawą o krajowym systemie cyberbezpieczeństwa, środki są również w innych resortach. Nie chciałbym, żebyśmy obszar cyber traktowali w sposób wybiórczy, z punktu widzenia wąskiej specjalizacji dotyczącej bezpieczeństwa czy Ministerstwa Obrony Narodowej. Szanowni państwo, wojska cybernetyczne są faktem. Mam na myśli chociażby Sojusz Północnoatlantycki. Norwegia jest prekursorem w tym obszarze, ale proszę pamiętać o tym, że dzięki determinacji rządu Prawa i Sprawiedliwości i ministra obrony narodowej Antoniego Macierewicza na agendzie szczytu NATO w Warszawie w 2016 r. obszar cyber był tak mocno eksponowany. Dzięki temu były konkretne ustalenia. To właśnie tu, w Warszawie zapadły decyzje, że wojska sojusznicze podejmują wyzwanie tworzenia swoich narodowych wojsk w obszarze cyber – w obszarze wojsk cybernetycznych. To jest ustalenie szczytu NATO w Warszawie. Bez wątpienia jest to jeden z sukcesów, które udało się osiągnąć na tym szczycie w 2016 r. Bardzo proszę o uzupełnienie mojej wypowiedzi pana dyrektora Dziubę oraz pana majora Iwaszko, jeśli chodzi o kwestie dotyczące informacji i przepływu informacji, bo Służba Kontrwywiadu Wojskowego ma w tym zakresie wiele ciekawych spostrzeżeń.

Zastępca dyrektora NCK Paweł Dziuba:

Dziękuję bardzo, panie ministrze. Panie przewodniczący, szanowni państwo, jeśli chodzi o środki finansowe, to w uzupełnieniu powiem, że do programu operacyjnego i do środków, które są przeznaczone na Narodowe Centrum Kryptologii, należy jeszcze dołączyć środki, które są przeznaczone na inwestycje. Myślę, że kwota, którą wspominał czy do której nawiązał w swoim wystąpieniu pan poseł Suski i pan ministerstw Macierewicz, jest realna, jeżeli weźmiemy pod uwagę inwestycje. Oczywiście…

Sekretarz stanu w MON Wojciech Skurkiewicz:

Przepraszam, panie dyrektorze, bo jest jeszcze jedna ważna kwestia do uzupełnienia. Niech państwo nie zapominają, że na przełomie 2015 r. i 2016 r. czy w 2016 r. byliśmy tak zdeterminowani co do obszaru cyberbezpieczeństwa, że wprowadziliśmy piętnasty program, jeżeli chodzi o programy modernizacji technicznej, który dotyczy właśnie cyberbezpieczeństwa. Program modernizacji technicznej sił zbrojnych na lata 2013–2022 obejmował 14 programów. Zdeterminowani, kładąc nacisk na obszar cyber, wprowadziliśmy piętnasty program, który dotyczy cyberbezpieczeństwa.

Zastępca dyrektora NCK Paweł Dziuba:

Szanowni państwo, jeszcze gwoli uzupełnienia powiem, że od 2016 r. jedna z istotnych uczelni, Wojskowa Akademia Techniczna, zwiększa swój nabór z kilkudziesięciu do kilkuset osób. W 2018 r. przyjęto ponad 800 kandydatów na podchorążych, czyli na przyszłych oficerów. To są takie działania systemowe, które związane są nie tylko z naborem, z korzystaniem z posiadanych kadr i z zachęcaniem osób funkcjonujących na rynku cywilnym. Podejmowane są również działania związane z tym, żeby wraz z kolejnymi absolwentami ten nabór wzrastał i zwiększał potencjał sił zbrojnych, czyli naszych Wojsk Obrony Cyberprzestrzeni. Dodatkowo chciałbym zaznaczyć, że rozpoczęto również współpracę z Wojskami Obrony Terytorialnej. Traktujemy to jako pewien początek drogi tych żołnierzy, którzy później, po zdobyciu doświadczenia i po odpowiednich szkoleniach będą zainteresowani kontynuowaniem służby w Wojskach Obrony Cyberprzestrzeni. Na pewno jest to działanie wielofrontowe, wielowątkowe. Zgadzam się z tym, że jeżeli spojrzymy tylko na jedno źródło zasilania, to rzeczywiście możemy stwierdzić, że może nam brakować żołnierzy w Wojskach Obrony Cyberprzestrzeni. Natomiast są to działania wielosystemowe, podjęte i realizowane od 2016 r.

Dodatkowo chciałbym wspomnieć, że w Narodowym Centrum Kryptologii realizowane są również programy, o których wspominałem. Są to programy badawcze mające na celu podniesienie zdolności sił zbrojnych do realizacji zadań w cyberprzestrzeni. Oczywiście, każdy z tych programów jest programem niejawnym. Stąd bardzo trudno jest mi o nich mówić, ale takie działania są podejmowane. Systemowo one również wspierają naszych żołnierzy. Faktem jest, że nie można spocząć na laurach. Każdy z państwa zdaje sobie z tego sprawę. Każdy dzień przynosi kolejne wyzwania. Rozwiązanie, które dzisiaj nas zabezpiecza, jutro może okazać się mniej skuteczne. Stąd też przez cały czas jest to praca typu *neverending story*. Codzienna, ciężka, trudna praca specjalistów w Narodowym Centrum Kryptologii.

Jeśli pan minister pozwoli, powiem jeszcze o wynagrodzeniach. Na pewno – jak wspomniałem – Ministerstwo Obrony Narodowej, kierownictwo ministerstwa zadbało o to, żeby obszar cyberbezpieczeństwa traktować priorytetowo. Priorytetowo, to znaczy, żeby również znalazły się odpowiednie osoby i odpowiednie środki finansowe na zatrudnienie specjalistów. Mogę powiedzieć, że takich specjalistów udaje się nam zatrudniać. Tacy specjaliści są. Tacy specjaliści pojawiają się w Narodowym Centrum Kryptologii, wspierając ten obszar, bardzo wrażliwy obszar, jeśli chodzi o cyberbezpieczeństwo, jeśli chodzi o kryptologię.

Sekretarz stanu w MON Wojciech Skurkiewicz:

Panie majorze, proszę.

Przedstawiciel Służby Kontrwywiadu Wojskowego mjr Borys Iwaszko:

Szanowni państwo, panie przewodniczący, w uzupełnieniu informacji przekazanej przez pana ministra i przez pana dyrektora Dziubę chciałbym powiedzieć tylko kilka słów na temat wojny informacyjnej, dezinformacji i cyberbezpieczeństwa. Według międzynarodowych ustaleń osób, które na co dzień pracują nad tzw. cyberbezpieczeństwem, cyberbezpieczeństwo jest zawężone do czynności quasi-technicznych nie tylko pasywnych, do działalności technicznej. I to nie ma nic wspólnego z wojną informacyjną i z dezinformacją. Podejrzewam, że wszyscy wiemy – jak tu siedzimy na tej sali – że nasz główny adwersarz – Federacja Rosyjska – nie przewiduje w doktrynie wojennej niedziel ani nie oddziela czasu pokoju od czasu wojny. Przez cały czas mamy do czynienia z tzw. małą wojną, która w doktrynie Federacji Rosyjskiej prowadzona jest każdą możliwą metodą, m.in. także poprzez informacje.

Dezinformacje wykrywa i przeciwdziała im wyspecjalizowana jednostka wojskowa. To, co można o tym powiedzieć, na pewno przekaże państwu pan pułkownik Gładysz, ze względu na to, że ta jednostka pozostaje w jego gestii. Natomiast jeżeli chodzi o działania techniczne w cyberprzestrzeni, które nazywamy cyberbezpieczeństwem, to cały świat, a właściwie doktryna NATO mówi o tym, że robimy cyberbezpieczeństwo, czyli cyberobronę. Natomiast z cyberobrony możemy wydzielić coś, co nazywamy aktywną cyberobroną. O tych działaniach nie możemy mówić ze względu na klauzulę, którą jest

objęte posiedzenie Komisji. Takich informacji możemy ewentualnie udzielić w innej formie, ale na pewno – niestety – nie w dniu dzisiejszym.

Jeżeli chodzi o całą definicję i o całe spektrum, to wszystko, co wchodzi w cyberbezpieczeństwo, to obrona i aktywna obrona. Wojska, które powstają i które z czasem osiągną zdolność operacyjną, na pewno zgodnie ze standardami NATO będą potrafiły wykonywać czynności związane z obroną i aktywną obroną. Dziękuję.

Przewodniczący poseł Michał Jach (PiS):

Pan pułkownik Gładysz. Czy tak?

Zastępca szefa Zarządu Kierowania i Dowodzenia P-6 Sztabu Generalnego Wojska Polskiego płk Marek Gładysz:

Panie przewodniczący, szanowni państwo, ja w kwestii uzupełnienia informacji odnośnie do działań informacyjnych. Informacja, to jest coś innego niż cyber. To trzeba bardzo wyraźnie zrozumieć i rozróżnić. Mamy obecnie cztery domeny walki. Są to domeny: lądowa, powietrzna, morska oraz zgodnie z postanowieniem szczytu NATO cyberprzestrzeń. Cyberprzestrzeń jest domeną, czyli obszarem. Jeżeli mogę przywołać pewne porównanie, to w domenie lądowej karabin jest aktywnym narzędziem. W cyberprzestrzeni informacja jest właśnie takim karabinem, który musi przedostać się do obszaru cyber. Dlatego te rzeczy trzeba rozróżniać. Czymś innym jest kształcenie specjalistów, którzy będą w stanie zrozumieć informację, zrozumieć fake newsa, zrozumieć obszar, który może być zakłócony tą informacją, a czymś innym jest przestrzeń, w której ta informacja się porusza. Mogę jeszcze dodać, że oprócz tych dwóch aspektów – czyli cyber i informacja – należy jeszcze dodać efekt psychologiczny. Aktualnie siły zbrojne również w tym aspekcie posiadają pewne zdolności. Te zdolności są opisane w planach, o których – co do zasady – nie można tutaj w tej chwili powiedzieć. Dziękuję.

Sekretarz stanu w MON Wojciech Skurkiewicz:

Przepraszam, panie przewodniczący, tylko gwoli uzupełnienia. Jesteśmy również otwarci na dyskusję, jeżeli będą państwo tego chcieli. Na pewno będzie ona interesująca i poszerzająca naszą wiedzę, jeżeli będzie przeprowadzona w trybie niejawnym. Dlatego jesteśmy otwarci, żeby takie spotkanie przygotować, oczywiście, o ile wyrażą państwo taką wolę i ochotę. Jesteśmy do tego przygotowani. To zależy od państwa. Decyzja należy do państwa. W tym obszarze jest wiele informacji i kwestii wrażliwych, które nie mogą być omawiane przy otwartej kurtynie, na otwartym posiedzeniu Komisji.

Przewodniczący poseł Michał Jach (PiS):

To jest dobry okres, bo wkrótce będziemy przyjmować plan pracy na następne półrocze. Jeżeli będzie taka propozycja, to – oczywiście – możemy ją uwzględnić w planie pracy Komisji na kolejny okres. Pan minister Macierewicz chciał zabrać głos. Proszę bardzo.

Poseł Antoni Macierewicz (PiS):

Panie przewodniczący, panie ministrze, panowie oficerowie, szanowni państwo, mam dwa króciutkie uzupełnienia. Ponieważ ta problematyka jest względnie nowa, w świadomości społecznej, także w świadomości niektórych posłów, bywają problemy z terminologią i ze zrozumieniem istoty rzeczy. Szczyt NATO przyjął, że przestrzeń cybernetyczna jest obszarem działań operacyjnych, działań wojennych, nie ograniczając ich w żadnym przypadku do działań defensywnych. Zresztą z natury działań cybernetycznych takie ograniczenie byłoby niemożliwe. Zwrócił na to uwagę pan minister, a także pan major. Jest oczywiste, że zarówno sposób działania, jak i czas działania nie może być ograniczony w klasycznym tego słowa znaczeniu, co tworzy pewien problem prawny, z którym się borykaliśmy. Zapewne będziemy się z nim borykali jeszcze przez jakiś czas. To jest jedna uwaga.

Druga uwaga, o której chciałem bardzo jasno powiedzieć jest taka, że decyzja ministra obrony narodowej podjęta na podstawie strategicznego przeglądu obronnego przewidywała – dziękuję najmocniej za realizację tej decyzji – utworzenie wojsk cybernetycznych. Tyle – być może tutaj jest pewne nieporozumienie – że nie jako odrębny rodzaj wojsk sił zbrojnych. Wojska Rakietowe i Artylerii też nie są odrębnym rodzajem wojsk, a mimo

to mam nadzieję, że skutecznie działają, a wierzę, że jeszcze skuteczniej niż dotychczas. To samo dotyczy wojsk cybernetycznych. Dziękuję bardzo.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję. Proszę państwa, cyberbezpieczeństwo często jest mylone z dezinformacją. W ciekawy sposób powiedział o tym bodajże dwa lata temu były doradca prezydenta Regana. Powiedział, że po raz pierwszy mamy takie pokolenie, w czasie życia którego powstały dwa dodatkowe domeny w zakresie działań operacyjnych. Jest to kosmos i cyberprzestrzeń. Jak widać po przebiegu dyskusji cyberbezpieczeństwo odgrywa coraz ważniejszą rolę. Proszę bardzo, pani poseł Anna Maria Siarkowska.

Poseł Anna Maria Siarkowska (PiS):

Bardzo dziękuję. Panie przewodniczący, panie ministrze, Wysoka Komisjo, cieszę się, że pan minister Macierewicz wyjaśnił tę wątpliwość, że nie będzie to osobny rodzaj sił zbrojnych. W takim razie mam takie pytanie. Jakie podporządkowanie planuje się dla wojsk cybernetycznych? Czy planuje się, że będą bezpośrednio podporządkowane któremuś z rodzajów sił zbrojnych? Drugie pytanie jest tak naprawdę trochę szersze. Jest to swego rodzaju uwaga. Mówimy, że już dzisiaj wojsko podejmuje przeciwdziałania w walce informacyjnej, przeciwdziała w obszarze cyber. Patrząc na to, co dzieje się wokół sił zbrojnych, na to, jak są przedstawiane w mediach i jak często są upowszechniane fake newsy, które bardzo trudno odkłamać, tak naprawdę mam wątpliwości co do skuteczności tych działań.

Pozwolę sobie przywołać tutaj kilka przykładów. Pierwszy dotyczy materiału, który swego czasu wyemitowała telewizja TVN. Potem ten materiał był skorelowany z materiałem, który ukazał się w „Gazecie Wyborczej" pod tytułem „Dość bose Antki". Teoretycznie miał się odnosić do Wojsk Obrony Terytorialnej, a przynajmniej takie były sugestie. Jeśli ktoś wczytał się w ten artykuł lub uważnie obejrzał materiał filmowy, okazywało się, że kwestie związane z nowym rodzajem sił zbrojnych, z Wojskami Obrony Terytorialnej, były zupełnie pomieszane z kwestiami dotyczącymi organizacji proobronnych takich, jak np. „Strzelec". Ze swej natury takie organizacje nie są częścią sił zbrojnych. Mają zupełnie inaczej prowadzone szkolenie. Co jest naturalne, ćwiczą przy użyciu atrap broni, a nie normalnej broni, jak żołnierze funkcjonujący w siłach zbrojnych na strzelnicach czy poligonach, bo organizacje proobronne mają inny charakter. Tak wszystko było tak zmiksowane, tak podane, że ktoś, kto czytał artykuł lub oglądał wyemitowany materiał, miał poczucie, że jest w nich mowa o Wojskach Obrony Terytorialnej. Oczywiście, potem wiele innych mediów, w tym radio, powielało te nieprawdziwe materiały wyśmiewając Wojska Obrony Terytorialnej, jakoby ich żołnierze ćwiczyli z atrapami broni, co było kompletnym kłamstwem, kompletną nieprawdą. Myślę, że w dużej mierze ten materiał nie został odkłamany.

Następny przykład pochodzi z ostatnich dni. Warto tutaj przypomnieć sytuację, w której Rzeczpospolita opublikowała materiał dotyczący organizacji proobronnych i ich udziału w ćwiczeniach Anakonda oraz kwestii związanych z postrzeganiem organizacji proobronnych, które nie są częścią sił zbrojnych, przez naszych sojuszników, przez sojuszników amerykańskich. Oczywiście, były kwestie tego, że będą dalej ćwiczyć z atrapami broni. Ta informacja została podana przez inne media i portale internetowe w ten sposób, że czego to dotyczy? Tak. Dobrze się państwo domyślają. Że dotyczy Wojsk Obrony Terytorialnej. Że to Wojska Obrony Terytorialnej będą ćwiczyć z atrapami broni, że ten rodzaj sił zbrojnych jest niechętnie widziany przez sojuszników.

Szanowni państwo, trudno tego rodzaju sytuacje traktować jako przypadki, bo to powtarza się wiele razy. Jest to wymierzone stricte w dobre imię żołnierzy Wojsk Obrony Terytorialnej i w to, w jaki sposób Wojska Obrony Terytorialnej są postrzegane przez społeczeństwo. To jest pierwsza rzecz. A druga rzecz jest taka, co tak naprawdę robi wojsko? W jaki sposób przeciwdziała tego typu dezinformacjom? Mamy do czynienia z rozpowszechnianiem fake newsów i tak naprawdę z bardzo słabymi i nieefektywnymi – w moim odczuciu, w moim przekonaniu – działaniami, które odkłamywałyby tego typu informacje, bądź im zapobiegały. Bardzo dziękuję.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję, pani poseł. Czy są jeszcze jakieś pytania do pana ministra? Jeśli nie, to bardzo proszę, panie ministrze.

Sekretarz stanu w MON Wojciech Skurkiewicz:

Pani poseł, całkowicie zgadzam się z tym, co pani mówi.

Przewodniczący poseł Michał Jach (PiS):

Proszę państwa, następnym razem porozmawiamy o polskich gazetach. Ale teraz proszę pozwolić panu ministrowi odpowiedzieć na pytania. Bardzo proszę, panie ministrze.

Sekretarz stanu w MON Wojciech Skurkiewicz:

Szanowni państwo, dziś żyjemy w globalnej wiosce. Przenikanie tych informacji, a co za tym idzie fake newsów czy nieprawdziwych informacji jest czymś, co – niestety – jest na porządku dziennym. Bardzo często są to informacje, które przede wszystkim służą temu, żeby wprowadzać dezinformacje. One po prostu temu służą. Jeśli ktoś przygotowuje taki materiał, to ten materiał ma służyć wywołaniu zniechęcenia, zniecierpliwienia albo wręcz agresji w stosunku do określonej grupy, określonych osób czy określonego środowiska. To jest faktem. Dzisiaj, podejmując działania, musimy mieć pełną świadomość tego, że należy temu przeciwdziałać. Tylko nie ma idealnego rozwiązania, które pokazuje, jak temu przeciwdziałać.

Informacja, która dziś pojawia się w portalu społecznościowym, np. na Twitterze, w ciągu sekundy dociera do dziesiątków tysięcy czy nawet do milionów osób i później jest kolportowana dalej. Nawet sprostowanie tej informacji niewiele daje, bo ona idzie w świat. To jest problem. Dzisiaj musimy stwarzać mechanizmy odporne na działania, które będą uderzały bezpośrednio w konkretną instytucję czy w konkretne miejsce. I to jest przede wszystkim ważne, żeby nie dopuszczać do hackowania stron czy podszywania się pod konkretne strony, bo to też rodzi pewnego rodzaju niebezpieczeństwa. Informacja wysłana z fake'owego konta mającego w adresie wyraz „mon" jest dla wielu informacją objawioną, czytelną, a nawet informacją w formie rozkazu. A przecież jest to informacja wysłana z nieprawdziwego konta. Dzisiaj musimy temu przeciwdziałać, bo taka sytuacja może wprowadzać wiele zamieszania i prowadzić wielu niepotrzebnych i bardzo groźnych sytuacji. Panie dyrektorze, czy jeszcze pan?

Przewodniczący poseł Michał Jach (PiS):

Pani poseł, jeszcze momencik. Pan dyrektor uzupełni odpowiedź.

Zastępca dyrektora NCK Paweł Dziuba:

Szanowni państwo, w kwestii uzupełnienia odpowiedzi na pytanie o Wojska Obrony Cyberprzestrzeni. W pierwszej kolejności będą one podporządkowane pod ministra, a w drugiej pod szefa Sztabu Generalnego Wojska Polskiego, po osiągnięciu gotowości. To było pierwsze pytanie pani poseł. Jeśli chodzi o informacje, to – szanowni państwo – m.in. dzięki państwa pracy powstała ustawa o krajowym systemie cyberbezpieczeństwa. W ustawie trzy filary – MON, NASK i GOV – zostały zobowiązane do sprawowania dwudziestoczterogodzinnej kontroli nad tym, żeby szybko reagować również na aspekty związane z właściwym rozumieniem czy rozpowszechnianiem nieprawdziwych informacji. W resorcie obrony narodowej jest 24-godzinny dyżur. Staramy się prostować te informacje, jeżeli jest taka konieczność. Natomiast faktem jest to, o czym wspomniał pan minister. Trudno jest przy tak szybkim pączkowaniu, jakie obserwujemy przy używaniu Twittera czy innych mediów społecznościowych, coś odwrócić i powrócić do stanu początkowego, kiedy ta informacja już się rozeszła. Niestety, taki jest stan. Dziękuję bardzo.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję. Pani poseł Anna Sobecka. Bardzo proszę.

Poseł Anna Sobecka (PiS):

Dziękuję, panie przewodniczący. Szanowni państwo, chciałam tylko powiedzieć, że na takie sytuacje, o których mówiła pani poseł Siarkowska i pan minister, jest tylko jedno lekarstwo. To jest repolonizacja mediów. Wtedy media będą podawały właściwe

informacje. Axel Springer nie będzie nam robił polityki w Polsce. Uważam, że na te wszystkie fake newsy byłaby jedna rada – repolonizacja mediów. Dziękuję bardzo.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję. Pan minister Mroczek. Proszę.

Poseł Czesław Mroczek (PO):

Proszę państwa, po wypowiedziach niektórych posłów niebezpiecznie zbliżyliśmy się do takiej tezy, że największym zagrożeniem w cyberprzestrzeni w Polsce jest wolność słowa, w szczególności jeśli chodzi o wolność słowa związaną z wydawaniem gazet. Chcę wyraźnie powiedzieć, że tak sądzi mniejszość tej Komisji. Niech to się zapisze w protokole.

Przewodniczący poseł Michał Jach (PiS):

Czy jeszcze ktoś z państwa? Proszę bardzo, pan poseł Pudłowski.

Poseł Paweł Pudłowski (N):

Dziękuję. Panie przewodniczący, Wysoka Komisjo, myślę, że to jest w ogóle niezrozumienie tematu. To, co mówi pani posłanka o repolonizacji mediów nijak się ma do botów, do wykorzystania fake newsów, do stosowanego tak naprawdę przez inne siły rażenia w mediach tego, co dzieje się w Polsce. Po części sami jesteśmy winni, bo nie powołując się na konkrety powiem, że partie używają botów komunikacji, w popieraniu swoich tez, a więc to my tworzymy ten chaos, jako scena polityczna. I to jest do ogarnięcia.

Tak naprawdę nie padła odpowiedź na pytanie pani poseł Anny Siarkowskiej o to, co z tym robimy. Z jednej strony można zaakceptować to, że coś w sekundę rozchodzi się wśród tysięcy czy setek tysięcy osób. Ale, co z tego? Akceptujemy to? Nie. Muszą być źródła, które coś wiarygodnie podają. I trzeba eliminować boty. Trzeba eliminować strategie – również partyjne – polegające na tym, że wykorzystuje się fake konta do tego, żeby popularyzować jakieś informacje, żeby robić gdzieś szum, chaos czy sensację, kiedy jej nie ma.

Chciałbym jednak zaapelować do pana przewodniczącego o rozważenie możliwości odbycia posiedzenia Komisji w trybie niejawnym, bo to są ważne rzeczy mówiące o tym, jak mocno Polska podlega innym służbom w zakresie wykorzystania informacji i ich popularyzacji. Myślę, że bez względu na to, jak dużo pieniędzy byśmy nie zainwestowali, w sferze obrony software, bądź hardware i tak jesteśmy trochę skazani na pomoc Stanów Zjednoczonych – głównie – Izraela, bądź tych państw, z którymi polska armia współpracuje. Sami nie jesteśmy w stanie wypracować systemu pełnej odporności na takie ataki. Przypomnę raport, który powstał w 2015 r., przygotowany przez Najwyższą Izbę Kontroli. Ten raport nie pozostawił suchej nitki na tym, w jaki sposób realizujemy cyberobronę. Przypomnę też wypowiedź zdaje się, że z 2016 r., generała Bondaryka, który podaje konkretnie, w jaki sposób nasze systemy są otwarte i penetrowane m.in. przez służby rosyjskie. Apeluję o to, żeby odbyło się posiedzenie utajnione, na którym szczerze i otwarcie moglibyśmy porozmawiać o tym, jakie są szanse obrony, co robi polska armia, co może robić NASK, co może robić CERT, ABW itd., itd. Dziękuję.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję. Myślę, że w najbliższym czasie zajmie się tym prezydium Komisji, które zdecyduje, czy zajmiemy się tym jeszcze w tym roku, czy już w kolejnym, jak poprzednio mówiłem. Możemy to zrobić w następnym półroczu. Podejmiemy taką decyzję. Czy są jeszcze jakieś pytania do tematu posiedzenia? Nie ma. Czy pan minister ma jeszcze coś do powiedzenia? Nie.

W takim razie dziękuję państwu serdecznie. Słucham?

Poseł Anna Maria Siarkowska (PiS):

Mam pytanie niezwiązane z tematem posiedzenia.

Przewodniczący poseł Michał Jach (PiS):

To bardzo proszę, w ramach wolnych wniosków. Skoro zamknęliśmy już temat dzisiejszego posiedzenia, możliwe są jeszcze wolne wnioski. Proszę.

Poseł Anna Maria Siarkowska (PiS):

Bardzo dziękuję. Panie przewodniczący, Wysoka Komisjo, chciałabym zwrócić uwagę, że na poprzednich posiedzeniach ustaliliśmy, że bez zbędnej zwłoki spotkamy się, jako Komisja, z szefem Sztabu Generalnego Wojska Polskiego. W takim razie prosiłabym pana przewodniczącego o to, żeby umożliwił posłom z Komisji Obrony Narodowej spotkanie z szefem Sztabu Generalnego Wojska Polskiego po to, żebyśmy mogli z nim wreszcie spokojnie porozmawiać o najważniejszych sprawach dotyczących polskiej armii, w tym o cywilnej kontroli nad armią i obowiązkach, które zostały mu powierzone w nowo przyjętej ustawie. Bardzo dziękuję.

Przewodniczący poseł Michał Jach (PiS):

Pani poseł, ale powiedziałem wyraźnie, że poproszę szefa Sztabu Generalnego Wojska Polskiego na takie spotkanie w momencie, kiedy już będzie wiadomo, że nowelizacja tej ustawy wejdzie w życie. Dopóki pan prezydent tej ustawy nie podpisze, w moim przekonaniu trudno jest pytać szefa Sztabu Generalnego Wojska Polskiego o plany związane z jego działalnością w ramach nowych uregulowań dotyczących systemu kierowania i dowodzenia. Myślę, że szef sztabu już się do tego przygotowuje. Zadamy mu te pytania, kiedy pan prezydent podpisze ustawę. Pan prezydent ma chyba jeszcze ok. 10 dni na podpisanie tej ustawy. Jeśli ją podpisze, niezwłocznie zaproszę pana generała Andrzejczaka na nasze posiedzenie, jak tego sobie życzy Komisja. Czy tak może być? Czy jasno mówię?

Poseł Anna Maria Siarkowska (PiS):

Tak.

Przewodniczący poseł Michał Jach (PiS):

Dobrze. Jeżeli nie ma do mnie więcej pytań, dziękuję państwu. Zamykam posiedzenie Komisji.